UDC 342.9
DOI https://doi.org/10.32849/2663-5313/2023.9.05

Nataliia Serhiienko
Doctor of Legal Sciences,
Professor, Department of Public Law
Borys Grinchenko Kyiv University
18/2 Bulvarno-Kudriavska Street, Kyiv, Ukraine, 04053
n.serhiienko@kubg.edu.ua
ORCID ID: *0000-0001-8929-6743*

INFORMATION SECURITY AS A FUNDAMENTAL COMPONENT OF NATIONAL SECURITY

Abstract. ***Purpose.*** The purpose of this article is to examine the theoretical and methodological foundations of information security as a fundamental component of national security, which plays a key role in safeguarding national interests and the security of the state. ***Results.*** The article explores the essence of information security as a fundamental element of national security. The information domain is increasingly exposed to both external and internal threats, which, in most cases, pose risks to the interests of individuals, society, and the state. Information security, as an integral part of national security, plays a crucial role in the external and internal policies of the state and encompasses all areas of public life. The article examines the components of ensuring the state's information security and outlines the main areas of activity of governmental authorities. It defines the system for ensuring information security and highlights the features, functions, and operational aspects of its actors within the national security framework. The analysis covers the impact of information security on national security, the challenges posed by internal and external informational threats, protection of information, information sovereignty of the state, and information support. Conceptual approaches are proposed for ensuring information security and developing an information security system to support the proper functioning of the information space. This includes identifying and preventing threats to national security, the state, and its citizens in the information domain. ***Conclusions.*** The study concludes that the Information Security Strategy provides a normative basis for ensuring information security within the state's territory. However, it lacks provisions for economic security, leading to legal gaps and complications in the implementation of comprehensive information security. The field of information security is rapidly evolving and requires urgent regulatory improvement. It is essential to develop a legal framework to protect the rights and interests of the subjects and objects of information relations. The information domain must be based on reliable, complete, and timely information, as well as freedom of speech, in order to preserve and enhance the national information product within the global information space.

Key words: national security, information security, information protection, national security assurance, information, information leakage.

1. Introduction

In the national security system of the state, information security plays a crucial role, as it can significantly influence the resolution of domestic political, foreign policy, economic, and military conflicts. Inefficiencies in the organization of state authorities and civil society result in a broad spectrum of internal threats to the country's information security. The issue of legal gaps in the national information strategy is highly relevant; their refinement and amendment would substantially contribute to the successful resolution of challenges in the political, social, economic, and other domains of state activity.

The relevance of information security as a component of national security has been emphasized by leading scholars in the field of administrative law, including V.B. Averyanov, O.M. Bandurka, Yu.P. Bytyak, V.V. Halunko, I.P. Holosnichenko, O.Yu. Drozd, T.O. Kolomoiets, V.K. Kolpakov, A.T. Komziuk, V.A. Lipkan, O.M. Muzychuk, V.I. Kurylo, V.I. Olefir, S.P. Ponomariov, A.A. Starodubtsev, M.M. Tyshchenko, S.O. Shatrava, among others.

The purpose of this article is to examine the theoretical and methodological foundations of information security as a fundamental component of national security, which plays one of the key roles in ensuring the protection of vital national interests and the overall security of the state.

2. Information Security as a Component of National Security

One of the primary objectives of the state is ensuring the security of society, as the formation and development of human civilization have

always been closely linked with overcoming various internal and external political threats. National security cannot be viewed as an isolated or detached phenomenon from public life. Information support plays a particularly significant role in this context. At the current stage of societal development, a wide array of new information technologies, communication systems, and telecommunications infrastructure has emerged, making information a constant and essential attribute of state functioning. Informational influence on the state and society has become more effective than political, economic, or even military pressure.

Article 17 of the Constitution of Ukraine states: "The protection of the sovereignty and territorial integrity of Ukraine, the provision of its economic and information security, shall be the most important functions of the state and a matter of concern for all the Ukrainian people" (Constitution of Ukraine, 1996).

Thus, the term *"information"* is employed across various scientific and legal disciplines. It has acquired multiple meanings and is interpreted depending on the field of activity. According to the Law of Ukraine *On Information*, information is defined as any data and/or knowledge that can be stored on physical media or represented in electronic form (Law of Ukraine On Information, 1992).

A more comprehensive definition is offered in the *Legal Encyclopedia*: "Information" (from Latin *informatio* – explanation, representation, interpretation) is understood as data concerning individuals, objects, technologies, tools, resources, events, and phenomena occurring in all areas of state activity, public life, and the environment, regardless of the form in which such data are presented. This data may be expressed in the form of signals, symbols, sounds, moving or static images, or in any other way (Shemshuchenko, 1998).

The field of information security is governed by relevant normative legal acts, including: the Constitution of Ukraine, the Law of Ukraine *On Information*, the Law of Ukraine *On the National Informatization Program*, the Law of Ukraine *On National Security of Ukraine*, the Presidential Decree *On the Information Security Strategy*, the *Concept of National Security of Ukraine*, as well as applicable international standards.

It is appropriate to assert that information security, as a component of national security, represents a state of protection of vital interests of individuals, society, and the state, in which harm is prevented due to: incomplete, untimely, or unreliable information; negative informational influence; adverse effects of information technology use; unauthorized dissemination, use, and breaches of integrity, confidentiality, and availability of information (Sashchuk, 2019).

Modern scholar O.V. Lytvynenko defines information security as the protection of information, the safeguarding and control of the information space, and ensuring an adequate level of informational sufficiency (Lytvynenko, 1997, p. 10).

Researchers M.M. Prysiazhniuk and Ya.I. Bieloshevych characterize information security as a state of protection of vital interests of individuals, society, and the state, in which harm is prevented due to: incomplete, untimely, or unreliable information; negative informational influence; adverse consequences of the use of information technologies; unauthorized dissemination, use, and breaches of the integrity, confidentiality, and availability of information (Prysiazhniuk, Bieloshevych, 2013, p. 44).

B. Kormych rightly notes that information security is the state of protection of legally established norms and parameters of information processes and relations that ensure the necessary conditions for the existence of individuals, society, and the state as subjects of these processes and relations (Kormych, 2004, p. 92).

In the academic literature, various conceptual approaches to defining information security can be found. Some scholars consider it to be a multi-dimensional and multifaceted phenomenon affecting all spheres of public life, while others focus on the growing number of potential threats in the information space and the increasing destabilizing factors.

The Law of Ukraine *On the Concept of the National Informatization Program* defines information security as an essential component of national security. Thus, information security is recognized as an integral part of the political, economic, defense, and other sectors of national security. The objects of information security include information resources, channels of information exchange and electronic communication, mechanisms ensuring the functioning of electronic communication systems and networks, as well as other elements of the national information infrastructure. As a result of implementing the Program, a comprehensive set of regulatory documents will be developed addressing all aspects of the use of computing equipment for processing and storing restricted information; a set of national standards for documentation, maintenance, use, and certification of information protection software; a database of tools for diagnosing, localizing, and preventing viruses; new information protection technologies using spectral methods; and highly reliable cryptographic methods of information protection (Law of Ukraine On the Concept of the National Informatization Program, 1998).

The Law of Ukraine *On National Security of Ukraine*, which serves as a fundamental guide for ensuring Ukraine's national security, presents information security as a systemic and integral component of national security, albeit without a precise definition of the term (Law of Ukraine On National Security of Ukraine, 2018).

According to O.M. Kosohova and A.O. Siryk, who have studied the protection of the national information space in the context of hybrid warfare, several key destructive factors have been identified as having a damaging impact on Ukraine's information environment:

1. continuous personnel losses (casualties, prisoners, and wounded), which contribute to public distrust in Ukraine's military-political leadership, portraying it as unable to control the internal situation;

2. an inadequate national information security system that undermines patriotic sentiment;

3. the active dissemination of external information campaigns by the Russian Federation, which influence public opinion towards accepting a federal structure for Ukraine and resolving the conflict in the East under the terms of the Kremlin regime (Kosohov, Siryk, 2017, p. 39).

Information security is generally interpreted as the level of protection of information processes within the state. The current legislation establishes a range of legal and organizational measures aimed at securing the field of information security.

The main directions of the *Information Security Strategy of Ukraine* include: ensuring national information security, countering disinformation, and resisting information operations. The Strategy defines information security as a component of Ukraine's national security, representing a state of protection of state sovereignty, territorial integrity, democratic constitutional order, and other vital interests of the individual, society, and the state. This includes the proper assurance of constitutional rights and freedoms, such as the collection, storage, use, and dissemination of information; access to reliable and objective information; and the existence of an effective system of protection and counteraction to harmful informational influences — including coordinated dissemination of false information, destructive propaganda, other information operations, as well as unauthorized dissemination, use, and violations of the integrity of restricted-access information (Decree of the President of Ukraine On Information Security Strategy, 2021).

3. The Role of State Authorities in Ensuring Information Security

It is appropriate to highlight a distinct list of powers vested in state authorities regarding the assurance of information security, as the implementation of such powers plays a crucial role in safeguarding national security. The National Security and Defense Council of Ukraine operates in the information domain in accordance with the Constitution and laws of Ukraine. It coordinates the activities of executive authorities aimed at ensuring national security in the information sphere, particularly through the capacities of the Center for Countering Disinformation (Decree of the President of Ukraine On the Information Security Strategy, 2021).

The Cabinet of Ministers of Ukraine plays a leading role in the field of information security, ensuring the formation and implementation of state information policy, guaranteeing information sovereignty, allocating funding for programs related to information security, directing and coordinating the work of ministries and other executive bodies, and approving an action plan for implementing the Information Security Strategy.

The Ministry of Foreign Affairs of Ukraine, in the context of information security, contributes to the promotion and formation of a positive international image of Ukraine in global and foreign national information resources in order to protect its political, economic, and socio-cultural interests, reinforce national security, and restore the country's territorial integrity.

The Ministry of Defense of Ukraine, as a member of the National Security and Defense Council, is authorized to:

1. monitor the information environment and forecast and identify information threats to national security in the military sphere;

2. prepare and conduct information defense activities, coordinating the involvement of national security actors in these efforts;

3. develop and maintain the system of strategic communications of the defense forces;

4. carry out legal, organizational, technical, informational, and other actions to ensure its own information security, including the protection of the unified information environment of the defense forces, especially in deployment locations of military units and formations of the Armed Forces of Ukraine and other military entities established under Ukrainian law;

5. cooperate with domestic and foreign media outlets to report on national security and defense measures, as well as efforts to repel and deter armed aggression by the Russian Federation in Donetsk and Luhansk oblasts;

6. counter information operations and other information influence campaigns targeting the Armed Forces and other Ukrainian military formations;

7. deliver reliable information to members of the Armed Forces and other components of the defense forces (Decree of the President of Ukraine On the Information Security Strategy, 2021).

The Security Service of Ukraine (SSU) is designated by law as one of the main actors in ensuring national security. According to Article 17 of the Law of Ukraine *On National Security of Ukraine*, it is responsible for counterintelligence protection of state sovereignty, constitutional order, territorial integrity, defense and scientific-technical potential, cybersecurity, information security, and critical infrastructure (Law of Ukraine On National Security of Ukraine, 2018).

The SSU's activities in the area of information security are regulated by the following legislative acts: the Law of Ukraine *On the Security Service of Ukraine*, *On National Security of Ukraine*, *On Operative-Investigative Activity*, *On Counterintelligence Activities*, *On Combating Terrorism*, *On the Organizational and Legal Framework for Combating Organized Crime*, the *Information Security Strategy*, the *Cybersecurity Strategy of Ukraine*, as well as relevant international legal instruments. The SSU identifies, neutralizes, and mitigates threats to national security in the information domain within the scope of its authority.

In accordance with the Information Security Strategy, the main functions of the SSU in the information sphere include the special monitoring of domestic and foreign mass media and online platforms to detect threats to Ukraine's national security, and counteracting special information operations aimed at undermining the constitutional order, sovereignty, territorial integrity, or exacerbating socio-political and economic conditions (Decree of the President of Ukraine On the Information Security Strategy, 2021).

Ukrainian intelligence agencies, in the sphere of information security, safeguard national interests abroad and counter external information threats in the context of national defense and security.

Article 22 of the Law of Ukraine *On National Security of Ukraine* designates the State Service of Special Communications and Information Protection of Ukraine as the body responsible for the functioning and development of government communication systems, the National System of Confidential Communication, and for implementing state policy in areas such as cybersecurity of critical information infrastructure, state information resources and legally protected data, cryptographic and technical protection of information, telecommunications, use of the national radio frequency spectrum, special-purpose postal services, and government courier communications, among other statutory duties.

The National Council of Television and Radio Broadcasting of Ukraine is tasked with protecting Ukraine's information space from propagandist audiovisual content of the aggressor state and promoting Ukrainian broadcasting in the temporarily occupied territories (Decree of the President of Ukraine On the Information Security Strategy, 2021).

The powers of the Ministry of Internal Affairs of Ukraine in the area of information security are defined by the Resolution of the Cabinet of Ministers of Ukraine *On Approval of the Regulation on the Ministry of Internal Affairs of Ukraine* and by laws including *On National Security of Ukraine*, *On the National Police*, *On Operative-Investigative Activity*, and *On the Basic Principles of Ensuring Cybersecurity of Ukraine*.

The Ministry of Internal Affairs is a member of the National Security and Defense Council of Ukraine and acts as a stakeholder in the implementation of state information policy. It also cooperates with other national security entities to counter threats to national interests and national security.

The National Police of Ukraine ensures the protection of individual rights and freedoms, as well as public and state interests against cybercrime. It is responsible for preventing, detecting, suppressing, and solving cybercrimes, and raising public awareness about cybersecurity (Law of Ukraine On the Basic Principles of Cyber Security of Ukraine, 2017).

The Prosecutor's Office of Ukraine operates in accordance with the Constitution and the Law of Ukraine *On the Prosecutor's Office*. It forms a unified system responsible for:

1. maintaining public prosecution in court;
2. organizing and supervising pre-trial investigations, including overseeing covert investigative actions;
3. representing state interests in court in exceptional cases and as provided by law (Constitution of Ukraine, 1996).

Justice in Ukraine is administered exclusively by the courts, in accordance with Articles 124–125 of the Constitution of Ukraine and applicable laws. The courts adjudicate criminal offenses that threaten national security in the information domain.

Information security is of great importance not only for the state but also for the international community. The United Nations plays a significant role in global information security efforts by developing international legal frameworks to counteract the unlawful use of scientific and technological advances by terrorist

groups and organized crime. Issues of information security in the context of building a sustainable global information society are also actively addressed by several specialized UN agencies (Frolova, 2018, p. 4).

4. International Information Security

The United Nations defines international information security as a state of international relations that excludes violations of global stability and the creation of threats to the security of individual states and the global community within the information space (Dubov, Ozhevan, 2012, p. 61). New international documents were developed based on the UN resolutions "The Role of Science and Technology in the Context of International Security and Disarmament" and "Developments in the Field of Information and Telecommunications in the Context of International Security." These resolutions contain provisions concerning the use of emerging technologies in both civilian and military spheres, the application of modern scientific and technological advancements in weapons modernization, and the importance of countering destructive information influences (Kopiika, 2020, p. 103).

The primary goal of international organizations is security itself, with NATO having most effectively reformed its policy regarding information security. The organization has established centers in member states as multinational institutions for the development of digital security doctrines, the enhancement of intergovernmental cooperation, the implementation of theoretical findings into practical measures against digital threats, and the exchange of best practices in information protection among member and partner countries. Currently, NATO's Cyber Security Center operates in Estonia. It does not form part of NATO's military structure and is funded by sponsoring countries and NATO member states (Kononenko, Novikova, Kopytska, 2021).

Information security, as a component of national security, plays a vital role in identifying national interests and security priorities. The main threat to national security is the informational influence exerted on society by another state or actor, which poses risks to Ukraine's sovereignty, critical infrastructure, information resources, strategic communications, and public consciousness. Disinformation campaigns aim to impose an alternative system of values on the state and manipulate the behavior of its population for the benefit of the aggressor.

5. Conclusions

The Information Security Strategy outlines the regulatory framework for ensuring information security within the territory of the state. However, the legislator does not provide for the integration of economic security into the Information Security Strategy, which results in regulatory gaps and complicates the process of ensuring effective information security. The information security domain is dynamic and requires ongoing legal improvement. It is essential to develop a comprehensive regulatory framework aimed at protecting the rights and interests of the subjects and objects of informational relations.

The information environment must be built upon accurate, comprehensive, and timely information, while simultaneously upholding freedom of expression and fostering the development and preservation of national informational products in the global information space.

Responsibility for ensuring information security is currently distributed among various state authorities and law enforcement agencies. Therefore, it is necessary to establish a dedicated state body endowed with specific powers in the field of information security.

References

Constitution of Ukraine: dated June 28, 1996. (1996). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (in Ukrainian).

Law of Ukraine "On Information": dated October 2, 1992, No. 2657-XII. (1992). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian).

Shemshuchenko, Yu. S. (Ed.). (1998). *Yurydychna entsyklopediia* [Legal encyclopedia]. Kyiv: Ukrainska entsyklopediia (in Ukrainian).

Sashchuk, H. (2019). *Informatsiina bezpeka v systemi zabezpechennia natsionalnoi bezpeky* [Information security in the national security system]. *Journ. univ.kiev.ua*. Retrieved from http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php (in Ukrainian).

Lytvynenko, O. V. (1997). *Problemy zabezpechennia informatsiinoi bezpeky u postradianskykh krainakh* [Problems of ensuring information security in post-Soviet countries]. Extended abstract of candidate's thesis. Kyiv (in Ukrainian).

Prysiazhniuk, M. M., & Bieloshevych, Ya. I. (2013). *Informatsiina bezpeka Ukrainy v suchasnykh umovakh*[Information security of Ukraine in modern conditions]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky*, (30), 42–46 (in Ukrainian).

Kormych, B. A. (2004). *Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy* [Organizational and legal foundations of information security policy of Ukraine]. Doctoral thesis, Odesa (in Ukrainian).

Law of Ukraine "On the Concept of the National Informatization Program": dated February 4, 1998, No. 75/98-VR. (1998). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/75/98-вр#Text (in Ukrainian).

Law of Ukraine "On National Security of Ukraine": dated June 21, 2018, No. 2469-VIII. (2018). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text (in Ukrainian).

Kosohov, O. M., & Siryk, A. O. (2017). *Zavdannia zakhystu natsionalnoho informatsiinoho prostoru za dosvidom vedennia hibrydnoi viiny RF na Skhodi Ukrainy* [The task of protecting the national information space based on the experience of conducting a hybrid war of the Russian Federation in the East of Ukraine]. *Systemy ozbroiennia i viiskova tekhnika*, (2), 38–41 (in Ukrainian).

Decree of the President of Ukraine "On Information Security Strategy": dated December 28, 2021, No. 685/2021. (2021). *President of Ukraine*. Retrieved from https://www.president.gov.ua/documents/6852021-41069 (in Ukrainian).

Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine": dated October 5, 2017, No. 2163-VIII. (2017). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

Frolova, O. M. (2018). *Rol OON v systemi mizhnarodnoi informatsiinoi bezpeky* [The role of the UN in the system of international information security]. *Elektronne vydannia Instytutu mizhnarodnykh vidnosyn*, (18). Retrieved from http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (in Ukrainian).

Dubov, D. V., & Ozhevan, M. A. (2012). *Maibutnie kiberprostoru ta natsionalni interesy Ukrainy: novi mizhnarodni initsiatyvy providnykh heopolitychnykh hravtsiv: Analytichna dopovid* [The future of cyberspace and national interests of Ukraine: new international initiatives of leading geopolitical players: Analytical report]. Kyiv: NISD (in Ukrainian).

Kopiika, M. V. (2020). *Modernizatsiia polityky mizhnarodnykh orhanizatsii u sferi informatsiinoi bezpeky*[Modernization of international organizations' policy in the field of information security]. *Politychne zhyttia*, (1), 102–109 (in Ukrainian).

Kononenko, V. P., Novikova, L. V., & Kopytska, P. O. (2021). *Polityka mizhnarodnykh orhanizatsii z pytan informatsiinoi bezpeky* [Policy of international organizations on information security]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*, (65), 353–358 (in Ukrainian).

Наталія Сергієнко
доктор юридичних наук,
професор кафедри публічного права
Київського університету імені Бориса Грінченка
вул. Бульварно-Кудрявська, 18/2, м. Київ, Україна, 04053
n.serhiienko@kubg.edu.ua
ORCID ID: *0000-0001-8929-6743*

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ФУНДАМЕНТАЛЬНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Abstract. ***Purpose.*** Мета статті полягає дослідженні теоретико-методологічних основ інформаційної безпеки як фундаментальну складову національної безпеки, що відіграє одну з ключових ролей у забезпеченні національної безпеки та життєво важливих інтересів держави. ***Results.*** Стаття присвячена розкриттю сутності інформаційної безпеки як фундаментальної складової національної безпеки. В інформаційній сфері супроводжуються появи зовнішніх так і внутрішніх загроз, які в більшості випадків загрожують інтересам особистості, суспільства, держави та її національній безпеці. Інформаційна безпека як складова національній безпеці відіграє важливу роль є складовою зовнішньої і внутрішньої політики держави та охоплює всі сфери життєдіяльності суспільства. Розглянуто складові щодо забезпечення інформаційної безпеки держави та основні напрямки діяльності державних органів влади. Визначено систему забезпечення інформаційної безпеки та особливості функціонування та функції її субєктів у сфері національної безпеки. Проаналізовано вплив інформаційної безпеки на національну безпеку, а також проблеми внутрішніх та зовнішніх інформаційних загроз, захист інформації безпеки, інформаційного суверенітету держави та інформаційного забезпечення. Запропоновані концептуальні підходи щодо забезпечення інформаційної безпеки та системи інформаційної безпеки для належного функціонування інформаційного простору, з метою виявлення та попередження загроз національній безпеці, держави та її громадянам в інформаційній сфері.

Conclusions. Зроблено висновок, що в Стратегії інформаційної безпеки вбачаються нормативне закріплення щодо забезпечення інформаційної безпеки в межах території держави. Законодавець в Стратегії інформаційної безпеки не передбачає забезпеченні економічної безпеки, що призводить до нормативних прогалин та ускладнює забезпечення інформаційної безпеки. Сфера інформаційної безпеки постійно змінюється є нагальною і потребує нормативного вдосконалення. Слід розробити нормативну правову базу щодо забезпечення захисту прав та інтересів суб'єктів і об'єктів інформаційних відносин. Інформаційна сфера повинна будуватися на достовірній повній, своєчасній інформації та свободу слова щодо вдосконалення, збереження національного інформаційного продукту у світовому інформаційному просторі.

Ключові слова*: національна безпека, інформаційна безпека, інформаційний захист, забезпеченя національної безпеки, інформація, виток інформації.*